International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-10 Issue-01 August 2015

Ensuring the Security of Communications Using Cloud Data Through Authentication

ABSTRACT

One of the newer methods of computing, known as CLOUD computing, relies on networks that do not need hardware, allows for simultaneous and dispersed computation, is lucrative, and is structured around services. The advent of cloud computing has had far-reaching consequences for the information technology sector. In both academia and business, it plays a crucial role. Water, gas, electricity, and telephone are the four fundamental utilities that are already known to us. The use of the cloud ranks sixth among these conveniences.

Cloud computing is undeniably a great way to store data on the cloud, but it is important that the data we keep there is secure to prevent it from being misused or accessed by the wrong people.

Here, we provide a system that allows data consumers, auditors, and owners to all access the cloud from the same place using the same authentication method. This will help with a lot of things, such reducing costs and other capital expenditures, making the system run more efficiently, limiting its size, offering flexibility, operating in real time, and a lot more.

1. INTRODUCTION

Academic researchers and other cloud users have a lot to gain from cloud computing, but there are major security concerns that, if left unchecked, would reduce the technology's usefulness.

wide range of potential uses and applications.

The safety and confidentiality of the information kept in the cloud, rather than on physical servers, is the primary concern when it comes to cloud computing security. Data management is an additional critical issue. As a result of

Users of computer services entrust their data to commercial entities known as "cloud service providers" for storage and ad hoc use, with little to no assurance that the data would be adequately protected. The confidentiality of a company's proprietary information must be protected at all costs; else, serious repercussions may ensue.

it stored in the cloud must, therefore, be secure and available only to authorized users; in other words, it must not be made public. While this is necessary, it is not sufficient. In the concept of service-oriented cloud computing, the ability to have fine-grained access control and flexibility is highly sought. Take a school as an example. Its information system must ensure that only authorized personnel can access students' personal data and that only class instructors may view their grades. In this case, requirements set by the business or laws (like HIPAA) need access to and control over sensitive data. Cloud computing has made it feasible to do away with the need for users' computers to store data in addition to applications.

possessing any data or software at all on the machine.

2. HOW CLOUD COMPUTINGWORKS

2.1 BASIC COMPONENTS

- Resources: In cloud computing more than one user share theresources.
- Vast reach: Cloud computing can reach a large no. of systems.
- Flexibility: Resources can be increased and decreased as per therequirement.
- Payment: According to the resources used and time taken.

2.2 ARCHITECTURE OF CLOUDCOMPUTING

Cloud Computing Service Models

- **Cloud Software as a Service (SaaS):** Application and Information clouds, Use provider's applications over a network.
- **Cloud Platform as a Service (PaaS):** Development clouds, Deploy customer-created applications to acloud, cloud provider examplesWindows Azure, Google App Engine,Aptana Cloud.
- **Cloud Infrastructure as a Service (IaaS):** Clouds for

infrastructure, Processing of the rent, storing the data, capacity of the network, and many more computing assets.

Cloud computing deployment models

- **Private cloud:** Whereinfrastructure is shared for a specific group.
- **Public cloud:** Bought by the public.
- **Hybrid cloud:** Containing morethan one clouds.

2.3 CLOUD COMPUTING BENEFITS

Cloud computing offers lower computer costs. It also helps to achieve improved performance. Moreover, it reduces software costs, provides instant software updates, improved document format compatibility, unlimited storage capacity, device independence, and increased data reliability. It is beneficial in not only lowering the costs but also other capital expenses, increases the efficiency of the working of the system, constrains the size, offers flexibility, realtime working and much more.

Many profit based cloud computing systems have been built by different companies e.g., EC2 and S3 by Amazon, and Blue Cloud by IBM among the IaaS systems, Google App Engine and Yahoo Pig among the PaaS systems, and Apps and Sales force's Customer Relation Management (CRM) System by Googleamong the SaaS systems.

2.4 CLOUD COMPUTING DRAWBACKS

Requires a constant Internet connection,does not work well with low-speedconnections, can be slow, features mightbe limited, stored data might not be secure, and stored data can be lost.

2.5 CLOUD COMPUTING PROVIDERS

Amazon Web Services (AWS) -include Amazon S3, Amazon EC2, Amazon Simple-DB, Amazon SQS, Amazon FPS, and others. Salesforce.com - Delivers businesses over the internet using thesoftware as a service model. GoogleApps › Software-as-a-service for business email, information sharing and protection. And other providers Proof- point Sun Open Cloud Platform, Workday and etc.

3. PROBLEM DEFINITION

To ensure the data security in cloud computing environment. We aim to design a new security model for achieving following goals andobjectives.

- **Access Control:** In our proposed scheme, if a user wants to access a fileor the function then first he/she isrequired to get the privilege from theauthentication module. In our scheme,the authentication module will be the third party auditor. This third party auditor will be capable of authenticatingdata owner and the user of the data. This third party auditor will be appointed by the cloud service provider.
- **Authentication Data Security:**

In our proposed scheme, the authentication module will play an

USER AUTHENTICATION
DATA ENCRYPTION AND DATA PROTECTION
DATA DECRYPTION

Figure: Proposed Model

Earlier the data user, third party auditor

intermediates role. Neither the cloud service provider nor the user of the datawill be able to access the authentication data from it.

4. SOLUTION

We are proposing a novel 3-tier model to provide security to users data in cloud computing. The first tier isresponsible for data owner and user of cloud authentication. The second tier is responsible for encrypting data owner's data. It is also responsible for protectinguser's data from unauthorized access. The third tier is responsible for providing data decryption. It is shownbelow in figure:d data consumer used to be on different sites. the data owner uploaded the data on the cloud and sent it to third party auditor. The data consumer who used to be on a different site needed to authenticate itself in order to access the data. In our new model, the data owner, third party auditor and data consumer all will be on the same site. The dataowner will first need to login with itspre decided username and password and then it will be able to upload dataon the cloud. Similarly, the consumer will need to enter its pre-assigned username and password in order to download the data from the cloud.

5. ADVANTAGES

• Controlling Access: Our suggested system eliminates the need for users to get privilege from the authentication module in order to access certain files or functions. The authentication module serves as the impartial auditor in our plan. This independent auditor may verify the identity of both the data owner and the data user. Cloud service providers often use the services of independent auditors.

• Data Authentication: The authentication module acts as an intermediary in our suggested architecture. No one, not even the cloud provider or the data user, may access the authentication data stored there. WhyBoth the third-party auditor and the users' data would be stored on the same site under our suggested method. Consequently, compared to earlier techniques, the time needed for authentication and data encryption and decryption is reduced. Prior plans had the third party auditor and the data stored on different servers. In such instance, the time needed for verification is clearly going to be longer.

6. CONCLUSION

In our proposed scheme, the third party auditor and users data is on same site.So the time required for theauthentication purpose and dataencryption and decryption is less in comparison to previous schemes. Thus this scheme is more efficient with regard to time consumption.In previous schemes, the data and the third party auditor were on separate site. It is clear that in that case the time required for authentication will be more.This scheme will also require less costas all the operations will be carried out from the same site.

REFERENCES

1 Microsoft Azure, Web-Based

Web Services provided by Amazon, located at http://aws.amason.com.
[3] K. Konwinski, R. H. Katz, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, A. Fox, R. Griffith, A. D. Joseph [4] "Ensuring Data Storage Security in Cloud Computing through Two-way Handshake based on Token Management" (IEEE ART Com 2010), written by M. R. Tribhuwan, V. A. Bhuyar, and Shabana Pirzade.
[5]Article published in June 2012 in the International Journal of Electronics, Communication, and Computer Engineering, Volume 3, Issue 3, with the ISSN number 2249071X.

According to V. Sandhya's research published in the International Journal of Advanced Research in Computer Science (Volume 2, Issue 6, November–December 2011), there are many approaches to cloud computing security.
"Advance Cryptography Algorithm for Improving Data Security" (Vishwagupta, Gajendra Singh, & Ravindra Gupta, 2012), published in the International Journal of Advanced Research in Computer Science and Software Engineering, volume 2, issue 1, January 2012.
[8]. Cloud Computing Cryptography by Simarjeet Kaur
[9] The authors Birendra Goswani and Dr. S. N. Singh discuss how to use matrices and public key cryptography to strengthen cloud computing security in their article published in the International Journal of Engineering Research and Applications in July–August 2012, issue 4,

pages 339–344.
The number ten. In the International Journal of P2P Network Trends and Technology, G. Jai Arul Jose, C. Sanjeev, and Dr. C. Suyambulingom published an article titled "Implementation of Data Security in Cloud Computing" in 2011.